

DOCKET NO.: 266812US6PCT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Takehiko NAKANO, et al.

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HERewith

INTERNATIONAL APPLICATION NO.: PCT/JP04/09256

INTERNATIONAL FILING DATE: June 24, 2004

FOR: INFORMATION PROCESSING APPARATUS AND METHOD, RECORDING
MEDIUM AND PROGRAM

**REQUEST FOR PRIORITY UNDER 35 U.S.C. 119
AND THE INTERNATIONAL CONVENTION**

Commissioner for Patents
Alexandria, Virginia 22313

Sir:

In the matter of the above-identified application for patent, notice is hereby given that
the applicant claims as priority:

<u>COUNTRY</u>	<u>APPLICATION NO</u>	<u>DAY/MONTH/YEAR</u>
Japan	2003-281348	28 July 2003

Certified copies of the corresponding Convention application(s) were submitted to the
International Bureau in PCT Application No. PCT/JP04/09256. Receipt of the certified
copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been
acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Gregory J. Maier
Attorney of Record
Registration No. 25,599
Surinder Sachar
Registration No. 34,423

Customer Number

22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 08/03)

日本国特許庁
JAPAN PATENT OFFICE

24.06.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 2003年 7月28日

出願番号
Application Number: 特願2003-281348
[ST. 10/C]: [JP 2003-281348]

出願人
Applicant(s): ソニー株式会社

REC'D 15 JUL 2004

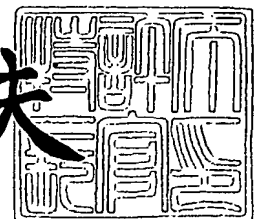
WIPO PCT

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2004年 4月28日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



BEST AVAILABLE COPY

【書類名】 特許願
【整理番号】 0390540408
【提出日】 平成15年 7月28日
【あて先】 特許庁長官殿
【国際特許分類】 H04L 9/00
【発明者】
 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内
 【氏名】 中野 雄彦
【特許出願人】
 【識別番号】 000002185
 【氏名又は名称】 ソニー株式会社
【代理人】
 【識別番号】 100082131
 【弁理士】
 【氏名又は名称】 稲本 義雄
 【電話番号】 03-3369-6479
【手数料の表示】
 【予納台帳番号】 032089
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9708842

【書類名】 特許請求の範囲**【請求項 1】**

受信装置と共有する共有データを、前記受信装置に送信する共有データ送信手段と、
前記受信装置において前記共有データに基づいて認証データが生成された後、応答を要求するコマンドを受信装置に送信するコマンド送信手段と、
前記共有データに基づいて生成された期待値と、前記受信装置において生成された前記認証データに基づいて前記受信装置を認証する認証手段と、
前記受信装置からの、前記コマンドに対する応答時間を計測する計測手段と、
前記認証手段による認証結果、および前記計測手段により計測された応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定手段と
を備えることを特徴とする情報処理装置。

【請求項 2】

前記コマンド送信手段は、データの送信可否を判定するのに、前記コマンドを最大N回送信し、
前記認証手段は、前記コマンドの送信の順番に応じた前記認証データとその前記期待値とに基づいて、前記受信装置を認証することを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】

受信装置と共有する共有データを、前記受信装置に送信する共有データ送信ステップと、
前記受信装置において前記共有データに基づいて認証データが生成された後、応答を要求するコマンドを受信装置に送信するコマンド送信ステップと、
前記共有データに基づいて生成された期待値と、前記受信装置において生成された前記認証データに基づいて前記受信装置を認証する認証ステップと、
前記受信装置からの、前記コマンドに対する応答時間を計測する計測ステップと、
前記認証ステップでの認証結果、および前記計測ステップの処理で計測された応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定ステップと
を含むことを特徴とする情報処理方法。

【請求項 4】

受信装置と共有する共有データの、前記受信装置に対する送信を制御する共有データ送信制御ステップと、
前記受信装置において前記共有データに基づいて認証データが生成された後の、応答を要求するコマンドの受信装置に対する送信を制御するコマンド送信制御ステップと、
前記共有データに基づいて生成された期待値と、前記受信装置において生成された前記認証データに基づく前記受信装置の認証を制御する認証制御ステップと、
前記受信装置からの、前記コマンドに対する応答時間の計測を制御する計測制御ステップと、
前記認証制御ステップでの認証結果、および前記計測制御ステップの処理で計測された応答時間に基づく、前記受信装置に対するデータの送信可否の判定を制御する判定制御ステップと
を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項 5】

受信装置と共有する共有データの、前記受信装置に対する送信を制御する共有データ送信制御ステップと、
前記受信装置において前記共有データに基づいて認証データが生成された後の、応答を要求するコマンドの受信装置に対する送信を制御するコマンド送信制御ステップと、
前記共有データに基づいて生成された期待値と、前記受信装置において生成された前記認証データに基づく前記受信装置の認証を制御する認証制御ステップと、
前記受信装置からの、前記コマンドに対する応答時間の計測を制御する計測制御ステッ

ブと、

前記認証制御ステップでの認証結果、および前記計測制御ステップの処理で計測された応答時間に基づく、前記受信装置に対するデータの送信可否の判定を制御する判定制御ステップと

を含む処理をコンピュータに実行させることを特徴とするプログラム。

【請求項 6】

送信装置と共有する共有データから生成された認証データに基づく認証結果、および前記送信装置からの所定のコマンドに対する応答時間に基づいてデータの送信可否を判定する前記送信装置と通信可能な情報処理装置において、

前記送信装置から前記コマンドが送信されてくる前に、前記共有データに対して所定の処理を施して、前記認証データを生成する認証データ生成手段と、

前記送信装置から前記コマンドが送信されてくる前に、前記認証データ生成手段により生成された前記認証データを含む、前記コマンドに対する応答メッセージを生成する応答メッセージ生成手段と、

前記送信装置から送信されてきた前記コマンドが受信されたとき、前記応答メッセージを前記送信装置に送信する送信手段と

を備えることを特徴とする情報処理装置。

【請求項 7】

前記共有データは、疑似乱数であり、

前記疑似乱数は、前記コマンドの前に前記送信装置から送信され、

前記認証データ生成手段は、前記疑似乱数に対して鍵付きハッシュ処理を施し、その結果得られたハッシュ値を前記認証データとする

ことを特徴とする請求項 6 に記載の情報処理装置。

【請求項 8】

前記認証データ生成手段は、前記疑似乱数と前記情報処理装置固有の情報に対して、鍵付きハッシュ処理を施し、その結果得られたハッシュ値を前記認証データとする

ことを特徴とする請求項 7 に記載の情報処理装置。

【請求項 9】

データの送信可否を判定するのに、前記送信装置から、前記コマンドが最大 N 回送信されてくる場合において、

前記認証データ生成手段は、前記送信装置から最初の前記コマンドが送信されてくる前に、前記共有データに対して前記処理を施して、送信されてくる N 個の前記コマンドのそれぞれに対応する N 個の前記認証データを生成し、

前記送信手段は、N 個の前記認証データが、前記送信装置と予め合意した順番で前記送信装置に提供されるように、前記応答メッセージ生成手段により生成された前記応答メッセージを前記送信装置に送信する

ことを特徴とする請求項 6 に記載の情報処理装置。

【請求項 10】

前記認証データ生成手段は、前記共有データに対して前記処理を施して得られたデータを複数個に分割し、分割されたデータから N 個の前記認証データを生成する

ことを特徴とする請求項 9 に記載の情報処理装置。

【請求項 11】

前記認証データ生成手段は、前記共有データに対して前記処理を繰り返し施し、その処理毎に得られたデータから、N 個の前記認証データを生成する

ことを特徴とする請求項 9 に記載の情報処理装置。

【請求項 12】

前記送信手段は、前記送信装置からの前記コマンドが受信されたとき、前記認証データと前記コマンドに含まれる情報から生成された新たな認証データを含む応答メッセージを、前記送信装置に送信する

ことを特徴とする請求項 6 に記載の情報処理装置。

【請求項 13】

送信装置と共有する共有データから生成された認証データに基づく認証結果、および前記送信装置からの所定のコマンドに対する応答時間に基づいてデータの送信可否を判定する前記送信装置と通信可能な情報処理装置の情報処理方法において、

前記送信装置から前記コマンドが送信されてくる前に、前記共有データに対して所定の処理を施して、前記認証データを生成する認証データ生成ステップと、

前記送信装置から前記コマンドが送信されてくる前に、前記認証データ生成ステップの処理で生成された前記認証データを含む、前記コマンドに対する応答メッセージを生成する応答メッセージ生成ステップと、

前記送信装置から送信されてきた前記コマンドが受信されたとき、前記応答メッセージを前記送信装置に送信する送信ステップと

を含むことを特徴とする情報処理方法。

【請求項 14】

送信装置と共有する共有データから生成された認証データに基づく認証結果、および前記送信装置からの所定のコマンドに対する応答時間に基づいてデータの送信可否を判定する前記送信装置と通信するためのプログラムであって、

前記送信装置から前記コマンドが送信されてくる前の、前記共有データに対して所定の処理を施しての前記認証データの生成を制御する認証データ生成制御ステップと、

前記送信装置から前記コマンドが送信されてくる前の、前記認証データ生成制御ステップの処理で生成された前記認証データを含む、前記コマンドに対する応答メッセージの生成を制御する応答メッセージ生成制御ステップと、

前記送信装置から送信されてきた前記コマンドが受信されたときの、前記応答メッセージの前記送信装置に対する送信を制御する送信制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項 15】

送信装置と共有する共有データから生成された認証データに基づく認証結果、および前記送信装置からの所定のコマンドに対する応答時間に基づいてデータの送信可否を判定する前記送信装置と通信するためのプログラムであって、

前記送信装置から前記コマンドが送信されてくる前の、前記共有データに対して所定の処理を施しての前記認証データの生成を制御する認証データ生成制御ステップと、

前記送信装置から前記コマンドが送信されてくる前の、前記認証データ生成制御ステップの処理で生成された前記認証データを含む、前記コマンドに対する応答メッセージの生成を制御する応答メッセージ生成制御ステップと、

前記送信装置から送信されてきた前記コマンドが受信されたときの、前記応答メッセージの前記送信装置に対する送信を制御する送信制御ステップと

を含む処理をコンピュータに実行させることを特徴とするプログラム。

【書類名】 明細書

【発明の名称】 情報処理装置および方法、記録媒体、並びにプログラム

【技術分野】

【0001】

本発明は、情報処理装置および方法、記録媒体、並びにプログラムに関し、特に、通信相手との通信時間を適切に計測することができるようにした情報処理装置および方法、記録媒体、並びにプログラムに関する。

【背景技術】

【0002】

近年、インターネットに代表される公共性のある広域に亘るネットワーク（以下、WAN(Wide Area Network)と記述する）や一般家屋等に設けられる局所的なネットワーク（以下、LAN(Local Area Network)と記述する）の普及に伴い、それらのネットワークを介した各種データ通信が盛んに行われている。その通信形態の1つとして、通信相手との通信距離に応じて通信を制御することが提案されている。例えば、コンテンツの不正配布を防止するために、同一のLANに接続されている端末（通信距離が短い端末）間においてのみデータの授受が可能となるように通信が制御される。

【発明の開示】

【発明が解決しようとする課題】

【0003】

ところで、このように通信相手との通信距離に応じて通信を制御する場合、通信距離を判別する（同一のLANに接続されているか否かを判定する）必要があるが、従来では、送信側が所定の要求に対する受信側からの応答時間を計測し、計測したその応答時間に基づいて通信距離を判別する方法が存在しなかった。

【0004】

本発明はこのような状況に鑑みてなされたものであり、応答時間を適切に計測し、その応答時間に基づいて通信距離を判別することを目的とする。

【課題を解決するための手段】

【0005】

本発明の第1の情報処理装置は、受信装置と共有する共有データを、受信装置に送信する共有データ送信手段と、受信装置において共有データに基づいて認証データが生成された後、応答を要求するコマンドを受信装置に送信するコマンド送信手段と、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づいて受信装置を認証する認証手段と、受信装置からの、コマンドに対する応答時間を計測する計測手段と、認証手段による認証結果、および計測手段により計測された応答時間に基づいて、受信装置に対するデータの送信可否を判定する判定手段とを備えることを特徴とする。

【0006】

コマンド送信手段は、データの送信可否を判定するのに、コマンドを最大N回送信し、認証手段は、コマンドの送信の順番に応じた認証データとその期待値とに基づいて、受信装置を認証することができる。

【0007】

本発明の第1の情報処理方法は、受信装置と共有する共有データを、受信装置に送信する共有データ送信ステップと、受信装置において共有データに基づいて認証データが生成された後、応答を要求するコマンドを受信装置に送信するコマンド送信ステップと、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づいて受信装置を認証する認証ステップと、受信装置からの、コマンドに対する応答時間を計測する計測ステップと、認証ステップでの認証結果、および計測ステップの処理で計測された応答時間に基づいて、受信装置に対するデータの送信可否を判定する判定ステップとを含むことを特徴とする。

【0008】

本発明の第1の記録媒体のプログラムは、受信装置と共有する共有データの、受信装置

に対する送信を制御する共有データ送信制御ステップと、受信装置において共有データに基づいて認証データが生成された後の、応答を要求するコマンドの受信装置に対する送信を制御するコマンド送信制御ステップと、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づく受信装置の認証を制御する認証制御ステップと、受信装置からの、コマンドに対する応答時間の計測を制御する計測制御ステップと、認証制御ステップでの認証結果、および計測制御ステップの処理で計測された応答時間に基づく、受信装置に対するデータの送信可否の判定を制御する判定制御ステップとを含むことを特徴とする。

【0009】

本発明の第1のプログラムは、受信装置と共有する共有データの、受信装置に対する送信を制御する共有データ送信制御ステップと、受信装置において共有データに基づいて認証データが生成された後の、応答を要求するコマンドの受信装置に対する送信を制御するコマンド送信制御ステップと、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づく受信装置の認証を制御する認証制御ステップと、受信装置からの、コマンドに対する応答時間の計測を制御する計測制御ステップと、認証制御ステップでの認証結果、および計測制御ステップの処理で計測された応答時間に基づく、受信装置に対するデータの送信可否の判定を制御する判定制御ステップとを含む処理をコンピュータに実行させることを特徴とする。

【0010】

本発明の第1の情報処理装置および方法、並びにプログラムにおいては、受信装置と共有する共有データが、受信装置に送信され、受信装置において共有データに基づいて認証データが生成された後、応答を要求するコマンドが受信装置に送信され、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づいて受信装置が認証され、受信装置からの、コマンドに対する応答時間が計測され、認証結果、および応答時間に基づいて、受信装置に対するデータの送信可否が判定される。

【0011】

本発明の第2の情報処理装置は、送信装置からコマンドが送信されてくる前に、共有データに対して所定の処理を施して、認証データを生成する認証データ生成手段と、送信装置からコマンドが送信されてくる前に、認証データ生成手段により生成された認証データを含む、コマンドに対する応答メッセージを生成する応答メッセージ生成手段と、送信装置から送信されてきたコマンドが受信されたとき、応答メッセージを送信装置に送信する送信手段とを備えることを特徴とする。

【0012】

共有データは、疑似乱数であるようにし、疑似乱数は、コマンドの前に送信装置から送信されるようにし、認証データ生成手段は、疑似乱数に対して鍵付きハッシュ処理を施し、その結果得られたハッシュ値を認証データとすることができる。

【0013】

認証データ生成手段は、疑似乱数と情報処理装置固有の情報に対して、鍵付きハッシュ処理を施し、その結果得られたハッシュ値を認証データとすることができる。

【0014】

データの送信可否を判定するのに、送信装置から、コマンドが最大N回送信されてくる場合において、認証データ生成手段は、送信装置から最初のコマンドが送信されてくる前に、共有データに対して処理を施して、送信されてくるN個のコマンドのそれぞれに対応するN個の認証データを生成し、送信手段は、N個の認証データが、送信装置と予め合意した順番で送信装置に提供されるように、応答メッセージ生成手段により生成された応答メッセージを送信装置に送信することができる。

【0015】

認証データ生成手段は、共有データに対して処理を施して得られたデータを複数個に分割し、分割されたデータからN個の認証データを生成することができる。

【0016】

認証データ生成手段は、共有データに対して処理を繰り返し施し、その処理毎に得られたデータから、N個の認証データを生成することができる。

【0017】

送信手段は、送信装置からのコマンドが受信されたとき、認証データとコマンドに含まれる情報から生成された新たな認証データを含む応答メッセージを、記送信装置に送信することができる。

【0018】

本発明の第2の情報処理方法は、送信装置からコマンドが送信されてくる前に、共有データに対して所定の処理を施して、認証データを生成する認証データ生成ステップと、送信装置からコマンドが送信されてくる前に、認証データ生成ステップの処理で生成された認証データを含む、コマンドに対する応答メッセージを生成する応答メッセージ生成ステップと、送信装置から送信されてきたコマンドが受信されたとき、応答メッセージを送信装置に送信する送信ステップとを含むことを特徴とする。

【0019】

本発明の第2の記録媒体のプログラムは、送信装置からコマンドが送信されてくる前の、共有データに対して所定の処理を施しての認証データの生成を制御する認証データ生成制御ステップと、送信装置からコマンドが送信されてくる前の、認証データ生成制御ステップの処理で生成された認証データを含む、コマンドに対する応答メッセージの生成を制御する応答メッセージ生成制御ステップと、送信装置から送信されてきたコマンドが受信されたときの、応答メッセージの送信装置に対する送信を制御する送信制御ステップとを含むことを特徴とする。

【0020】

本発明の第2のプログラムは、送信装置からコマンドが送信されてくる前の、共有データに対して所定の処理を施しての認証データの生成を制御する認証データ生成制御ステップと、送信装置からコマンドが送信されてくる前の、認証データ生成制御ステップの処理で生成された認証データを含む、コマンドに対する応答メッセージの生成を制御する応答メッセージ生成制御ステップと、送信装置から送信されてきたコマンドが受信されたときの、応答メッセージの送信装置に対する送信を制御する送信制御ステップとを含むことを特徴とする。

【発明の効果】

【0021】

第1の本発明によれば、受信装置の応答時間を適切に計測することができる。

【0022】

第2の本発明によれば、送信装置における応答時間の適切な計測に必要な情報を提供することができる。

【発明を実施するための最良の形態】

【0023】

以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【0024】

本発明の第1の情報処理装置は、受信装置と共有する共有データ（例えば、ランダムチャレンジ）を、受信装置に送信する共有データ送信手段（例えば、図3のランダムチャレンジ送信制御部32）と、受信装置において共有データに基づいて認証データが生成された後、応答を要求するコマンドを受信装置に送信するコマンド送信手段（例えば、図3のコマンド送信制御部34）と、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づいて受信装置を認証する認証手段（例えば、図3の判定部35）と、受信装置からの、コマンドに対する応答時間を計測する計測手段（例えば、図3の応答時間計測部36）と、認証手段による認証結果、および計測手段により計測さ

れた応答時間に基づいて、受信装置に対するデータの送信可否を判定する判定手段（例えば、図3の判定部35）とを備えることを特徴とする。

【0025】

コマンド送信手段は、データの送信可否を判定するのに、コマンドを最大N回送信し（例えば、図5のステップS6, 12; 13）、認証手段は、コマンドの送信の順番に応じた認証データとその期待値とに基づいて、受信装置を認証することができる（例えば、図5のステップS10）。

【0026】

本発明の第1の情報処理方法は、受信装置と共有する共有データを、受信装置に送信する共有データ送信ステップ（例えば、図5のステップS2）と、受信装置において共有データに基づいて認証データが生成された後、応答を要求するコマンドを受信装置に送信するコマンド送信ステップ（例えば、図5のステップS6）と、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づいて受信装置を認証する認証ステップ（例えば、図5のステップS10）と、受信装置からの、コマンドに対する応答時間を計測する計測ステップ（例えば、図5のステップS7, S9）と、認証ステップでの認証結果、および計測ステップの処理で計測された応答時間に基づいて、受信装置に対するデータの送信可否を判定する判定ステップ（例えば、図5のステップS11, S14, S15）とを含むことを特徴とする。

【0027】

本発明の第2の情報処理装置は、送信装置からコマンドが送信されてくる前に、共有データに対して所定の処理を施して、認証データを生成する認証データ生成手段（例えば、図4の認証データ生成部42）と、送信装置からコマンドが送信されてくる前に、認証データ生成手段により生成された認証データを含む、コマンドに対する応答メッセージを生成する応答メッセージ生成手段（例えば、図4の応答メッセージ生成部43）と、送信装置から送信されてきたコマンドが受信されたとき、応答メッセージを送信装置に送信する送信手段（例えば、応答メッセージ送信制御部44）とを備えることを特徴とする。

【0028】

共有データは、疑似乱数（例えば、ランダムチャレンジ）であるようにし、疑似乱数は、コマンドの前に送信装置から送信されるようにし（例えば、図5のステップS2）、認証データ生成手段は、疑似乱数に対して鍵付きハッシュ処理（例えば、HMAC（RFC 2104）アルゴリズムによるハッシュ処理）を施し、その結果得られたハッシュ値を認証データとすることができる。

【0029】

認証データ生成手段は、疑似乱数と情報処理装置固有（例えば、端末11の機器ID）の情報に対して、鍵付きハッシュ処理を施し、その結果得られたハッシュ値を認証データとすることができる。

【0030】

データの送信可否を判定するのに、送信装置から、コマンドが最大N回送信されてくる場合において、認証データ生成手段は、送信装置から最初のコマンドが送信されてくる前に、共有データに対して処理を施して、送信されてくるN個のコマンドのそれぞれに対応するN個の認証データを生成し（例えば、図5のステップS22）、送信手段は、N個の認証データが、送信装置と予め合意した順番で送信装置に提供されるように、応答メッセージ生成手段により生成された応答メッセージを送信装置に送信することができる（例えば、図5のステップS27）。

【0031】

認証データ生成手段は、共有データに対して処理を施して得られたデータを複数個に分割し、分割されたデータからN個の認証データ（例えば、図6に示す期待値と同様に生成された認証データ）を生成することができる。

【0032】

認証データ生成手段は、共有データに対して処理を繰り返し施し、その処理毎に得られ

たデータから、N個の認証データ（例えば、図7に示す期待値と同様に生成された認証データ）を生成することができる。

【0033】

送信手段は、送信装置からのコマンドが受信されたとき、認証データとコマンドに含まれる情報から生成された新たな認証データを含む応答メッセージを、記送信装置に送信することができる（例えば、図5のステップS27）。

【0034】

本発明の第2の情報処理方法は、送信装置からコマンドが送信されてくる前に、共有データに対して所定の処理を施して、認証データを生成する認証データ生成ステップと（例えば、図5のステップS22）、送信装置からコマンドが送信されてくる前に、認証データ生成ステップの処理で生成された認証データを含む、コマンドに対する応答メッセージを生成する応答メッセージ生成ステップ（例えば、図5のステップS25）と、送信装置から送信されてきたコマンドが受信されたとき、応答メッセージを送信装置に送信する送信ステップ（例えば、図5のステップS27）とを含むことを特徴とする。

【0035】

図1は、本発明を適用した端末11からなる情報通信システムの構成例を示している。

【0036】

LAN1-1、1-2（以下、個々に区別する必要がない場合、単位、LAN1と称する。他の場合についても同様である）がインターネットに代表されるWAN2を介して相互に接続されている。

【0037】

LAN1-1は、例えば、家屋内に設けられ、特定の個人（あるいは、家族）が使用する程度の規模のものであり、それには、スイッチングハブ（図示せず）を介して、パーソナルコンピュータやAV機器等の端末11-1および端末11-2が接続されている。LAN1-1と端末11-1および11-2との接続は、例えば、Ethernet(R) (100BASE-TX)等の高速インタフェースによる。端末11-1および11-2は、LAN1-1およびWAN2を介して、LAN1-2に接続することができる。

【0038】

LAN1-2は、LAN1-1と同様に構成されており、それには、端末11-3が接続されている。

【0039】

各端末11は、本情報通信システムに登録された正規の機器であり、図2に示すように、送信可否判定部21、応答制御部22、通信部23、および送信データ格納部24を含んで構成されている。

【0040】

送信可否判定部21は、他の端末11（受信側の端末11）に所定のデータを送信する際に、通信部23を介して、受信側の端末11（正確には、その応答制御部22）と後述するように通信することで、受信側の端末11が本情報通信システムにおける正規の機器であるか否かを認証するとともに、所定の要求に対する受信側の端末11の応答時間を、受信側の端末11との通信時間として計測する。

【0041】

送信可否判定部21は、受信側の端末11の認証結果および応答時間に基づく通信距離の判別結果に基づいて、受信側の端末11に対するデータの送信可否を判定する。

【0042】

例えば、受信側の端末11が、送信側の端末11と異なるLAN1に接続されている場合（WAN2を介して接続され、いわゆる通信距離が長い場合）、応答時間は、同じLAN1に接続されている場合（通信距離が短い場合）に比べて長くなるので、例えば、通信が同一LAN1内に制限されているとき、送信可否判定部21は、計測した応答時間から受信側の端末11が送信側の端末11と同じLAN1に接続されているか否かを判定し、その判定結果と受信側の端末11の認証結果に基づいて、データ送信の可否を判定する。

【0043】

すなわち図1の例では、端末11-1（送信側）が端末11-2（受信側）にデータを送信する場合、端末11-1の送信可否判定部21は、計測した端末11-2の応答時間から、端末11-2がLAN1-1に接続されていることを判定し、データ送信を行う。一方、端末11-1が端末11-3にデータを送信する場合、端末11-1の送信可否判定部21は、計測した端末11-3の応答時間から、端末11-3はLAN1-1と異なるLAN（LAN1-2）に接続されていることを判定し、データ送信を行わない。

【0044】

なおこのような通信距離による通信制御は、映画などのコンテンツを一定の地域に対して先行配給し、他の地域には後日配給するなどのコンテンツ配給ビジネスに適用することができる。

【0045】

図2に戻り、応答制御部22は、送信側の端末11から所定のデータの送信を受ける際、通信部23を介して、送信側の端末11（正確には、その送信可否判定部21）と後述するように通信することで、送信側の端末11における認証および応答時間の適切な計測に必要な情報を送信側の端末11に送信する。

【0046】

通信部23は、LAN1に接続されており、同一のLAN1内の端末11、またはWAN2を介して異なるLAN1に接続されている端末11との通信を行う。

【0047】

送信データ格納部24は、受信側の端末11に送信される、所定のデータが格納されている。

【0048】

図3は、端末11の送信可否判定部21の構成例を示している。

【0049】

ランダムチャレンジ生成部31は、所定ビット数の疑似乱数（以下、ランダムチャレンジと称する）を生成し、ランダムチャレンジ送信制御部32および期待値生成部33に供給する。

【0050】

ランダムチャレンジ送信制御部32は、ランダムチャレンジ生成部31から供給されたランダムチャレンジを、通信部23を介して、受信側の端末11に送信する。ランダムチャレンジ送信制御部32はまた、通信部23を介して、受信側の端末11から送信されてきた、ランダムチャレンジを受信した旨のメッセージ（以下、RC受信メッセージと称する）を受信し、そのときRC受信メッセージを受信した旨をコマンド送信制御部34に通知する。

【0051】

期待値生成部33は、ランダムチャレンジ生成部31から供給されたランダムチャレンジに対して、例えば、受信側の端末11と共有する秘密鍵を利用したHMAC（RFC 2104）アルゴリズムによるハッシュ処理（いわゆる鍵付きハッシュ処理）を施して、受信側の端末11でランダムチャレンジから生成される認証データの期待値を生成し、判定部35に供給する。期待値生成部33はまた、端末11に予め設定された端末11固有の情報（例えば、機器ID）とランダムチャレンジを連結したものに鍵付きハッシュ処理を施して期待値を生成することもできる。

【0052】

なお、ハッシュ処理で利用される秘密鍵は、本情報通信システムの正規の機器に所定のタイミングで安全に配信される。

【0053】

コマンド送信制御部34は、ランダム送信制御部32から、RC受信メッセージを受信した旨が通知されたとき、または判定部35からの指示に従って、応答を要求するコマンド（以下、応答要求コマンドと称する）を、通信部23を介して、受信側の端末11に送

信する。

【0054】

コマンド送信制御部34または、通信部23を介して、送信した応答要求コマンドに対する応答として、受信側の端末11から送信されてきたメッセージ（以下、応答メッセージと称する）を受信し、それを判定部35に供給する。応答メッセージには、ランダムチャレンジ送信制御部32により送信されたランダムチャレンジから生成された認証データが組み込まれている。

【0055】

コマンド送信制御部34または、応答要求コマンドを送信した後、応答時間計測部36を制御して、応答時間の計測を開始させるとともに、その応答要求コマンドに対する応答としての応答メッセージを受信したとき、応答時間の計測を終了させる。

【0056】

判定部35は、コマンド送信制御部34からの応答メッセージに組み込まれている認証データと、期待値生成部33で生成されたその認証データの期待値に基づいて、受信側の端末11が、本情報通信システムにおける正規の機器であるかの認証を行う。判定部35はまた、応答時間計測部36で計測された応答時間が所定の時間Xを越えているか否かを判定して、通信距離の判別（送信側の端末11と同一のLAN1に接続されているかの判定）を行う。

【0057】

判定部35は、受信側の端末11の認証結果および通信距離の判別結果に基づいて、データの送信可否の判定を行う。判定部35は、その判定結果に基づいて、通信部23を制御し、送信データ格納部24に格納されているデータを、受信側の端末11に送信させる。

【0058】

応答時間計測部36は、コマンド送信制御部34からの指示に従って、内蔵するタイマを動作させ、受信側の端末11の応答時間を計測する。

【0059】

図4は、端末11の応答制御部22の構成例を示している。

【0060】

ランダムチャレンジ受信制御部41は、通信部23を介して、送信側の端末11（正確には、その送信可否判定部21）から送信されてきたランダムチャレンジを受信し、それを認証データ生成部42に供給する。ランダムチャレンジ受信制御部41はまた、通信部23を介して、RC受信メッセージ（ランダムチャレンジを受信した旨を表すメッセージ）を、送信側の端末11に送信し、そのときRC受信メッセージを送信した旨を応答メッセージ送信制御部44に通知する。

【0061】

認証データ生成部42は、ランダムチャレンジ受信制御部41から供給されたランダムチャレンジに対して、送信側の端末11（送信可否判定部21の期待値生成部33）における場合と同様の鍵付きハッシュ処理を施して、第三者が予測できない認証データを生成し、応答メッセージ生成部43に供給する。

【0062】

応答メッセージ生成部43は、応答メッセージ送信制御部44の制御に従って、認証データ生成部42から供給された認証データを組み込んだ応答メッセージを生成し、応答メッセージ送信制御部44に供給する。

【0063】

応答メッセージ送信制御部44は、通信部23を介して、送信側の端末11から送信されてきた応答要求コマンドを受信する。

【0064】

応答メッセージ送信制御部44は、応答要求コマンドを受信する前のタイミングで（送信側の端末11から応答要求コマンドが送信されてくる前のタイミングで）、応答メッセ

ージ生成部 43 を制御して、受信する応答要求コマンドに対応した認証データが組み込まれた応答メッセージを生成させるとともに、応答要求コマンドを受信したとき、通信部 23 を介して、その応答メッセージを送信先の端末 11 に送信する。

【0065】

次に、図 5 のフローチャートを参照して、送信可否判定処理を行う場合の端末 11 の送信可否判定部 21 (図 2, 3) の動作を説明する。

【0066】

ステップ S1 において、端末 11 (送信側の端末 11) の送信可否判定部 21 のランダムチャレンジ生成部 31 は、ランダムチャレンジを生成し、それをランダムチャレンジ送信制御部 32 および期待値生成部 33 に供給する。

【0067】

ステップ S2 において、ランダムチャレンジ送信制御部 32 は、供給されたランダムチャレンジを、通信部 23 を介して受信側の端末 11 に送信し、ステップ S3 において、期待値生成部 33 は、供給されたランダムチャレンジに対して鍵付きハッシュ処理を施して、受信側の端末 11 で生成される認証データの期待値を生成する。

【0068】

なおこの例の場合、送信側の端末 11 は、データ送信の可否を判定するのに、最大 N (= 1, 2, . . .) 回応答要求コマンドを送信するので、ここでは、送信され得る N 個の応答要求コマンドに応じた認証データの N 個の期待値が生成される。

【0069】

N 個の期待値は、例えば、ランダムチャレンジに対して鍵付きハッシュ処理を施した結果得られたデータを複数個に分割し、その分割して得られたデータから N 個の期待値を生成することができる。図 6 の例の場合、ランダムチャレンジに対して鍵付きハッシュ処理を施した結果得られたデータが、N 個に分割されて、N 個の期待値 1 乃至期待値 N が生成される。

【0070】

また、ランダムチャレンジに対する鍵付きハッシュ処理を、複数回繰り返して行い、その処理毎に得られたデータから、N 個の期待値を生成することができる。図 7 の例の場合、ランダムチャレンジに対する鍵付きハッシュ処理が N 回繰り返して行われ、その処理毎に得られた N 個のデータが期待値となる。図 7 中、期待値 1 は、ランダムチャレンジに鍵付きハッシュ処理が 1 回施された結果得られたものであり、期待値 2 は、期待値 1 に、鍵付きハッシュ処理がさらに施された結果得られたものである。

【0071】

図 5 に戻り、ステップ S4 において、ランダムチャレンジ送信制御部 32 は、後述するように受信側の端末 11 から送信されてきた、ステップ S2 で送信されたランダムチャレンジを受信した旨を示す RC 受信メッセージを (ステップ S23)、通信部 23 を介して受信し、その旨をコマンド送信制御部 34 に通知する。ステップ S5 において、コマンド送信制御部 34 は、応答要求コマンドが何番目に送信されるものか (送信の順番) を示すカウンタ i に 1 を初期設定する。

【0072】

次に、ステップ S6 において、コマンド送信制御部 34 は、通信部 23 を介して、応答要求コマンドを受信側の端末 11 に送信し、ステップ S7 において、応答時間計測部 36 を制御して、応答時間の計測を開始させる。

【0073】

ステップ S8 において、コマンド送信制御部 34 は、後述するように受信側の端末 11 から送信されてきた、ステップ S6 で送信された応答要求コマンドに対する応答しての応答メッセージを、通信部 23 を介して受信して、判定部 35 に供給し、ステップ S9 において、応答時間計測部 36 を制御して、応答時間の計測を終了させる。すなわちステップ S7 で開始しステップ S9 で終了する時間計測で得られた時間が受信側の端末 11 の応答時間となる。

【0074】

ステップS10において、判定部35は、コマンド送信制御部34から供給された応答メッセージに組み込まれている認証データと、期待値生成部33により生成された、その認証データの期待値（具体的には、カウンタ*i*が示す順番に送信された応答要求コマンド（以下、第*i*番目に送信された応答要求コマンドと称する）に対応する期待値）とが一致するか否かを判定し、一致すると判定した場合、受信側の端末11を、情報通信システムにおける正規の端末であると認証し、ステップS11に進む。

【0075】

ステップS11において、判定部35は、応答時間計測部3で計測された、第*i*番目に送信された応答要求コマンドに対する受信側の端末11の応答時間が所定の時間Xを越えているか否かを判定する。時間Xは、例えば、同一LAN1に接続された端末11間で要する通信時間である。すなわち応答時間が時間Xを越える場合、受信側の端末11は、送信側の端末11と異なるLAN1に接続され、また、時間Xを越えない場合（応答時間＝時間Xを含む）、同一のLAN1に接続されていると判定することができる（通信距離を判別することができる）。

【0076】

ステップS11で、時間Xを越えると判定された場合、ステップS12に進み、判定部35は、その結果を、コマンド送信制御部34に通知し、コマンド送信制御部34はそのとき、カウンタ*i*を1だけインクリメントする。

【0077】

ステップS13において、コマンド送信制御部34は、カウンタ*i*＝N＋1であるか否かを判定する。ステップS13で、カウンタ*i*＝N＋1であると判定されたとき（すなわち、応答要求コマンドの送信がN回行われたとき）、またはステップS10で、受信側の端末11が本情報通信システムにおける正規の機器ではないと判定されたとき、ステップS14に進み、その旨を、判定部35に通知する。判定部35はそのとき、受信側の端末11へのデータ送信を不可とし、通信部23を制御して、送信データ格納部24に格納されているデータの受信側の端末11に対する送信を禁止する。

【0078】

ステップS11で、第*i*番目に送信された応答要求コマンドに対する応答時間が、時間Xを越えないと判定された場合、すなわち、受信側の端末11が、本情報通信システムにおける正規の機器であり、かつ、例えば送信側の端末11と同じLAN1に接続されている端末11であるとき、ステップS15に進み、判定部35は、通信部23を制御して、送信データ格納部24に格納されているデータを、受信側の端末11に送信させる。

【0079】

ステップS14またはステップS15で、受信側の端末11に対するデータ送信可否が判定されたとき、判定部35は、通信部23を介して、送信可否判定が終了した旨を表すメッセージ（以下、判定終了メッセージと称する）を受信側の端末11に送信する。その後、送信可否判定処理は、処理を終了する。

【0080】

次に、図5のフローチャートを参照して、応答処理を行う場合の端末11の応答制御部22（図2，4）の動作を説明する。

【0081】

ステップS21において、端末11（受信側の端末11）の応答制御部22のランダムチャレンジ受信制御部41は、送信先の端末11から送信されてきたランダムチャレンジを（ステップS2）、通信部23を介して受信し、認証データ生成部42に供給する。ステップS22において、認証データ生成部42は、ランダムチャレンジ受信制御部41から供給されたランダムチャレンジに対して、送信側の端末11の送信可否判定部21（期待値生成部33）における鍵付きハッシュ処理（ステップS3）と同様の鍵付きハッシュ処理を施し、認証データを生成し、応答メッセージ生成部43に供給する。

【0082】

なおこの例では、最大N個の応答要求コマンドを受信し得るので、その応答要求コマンドに対応する期待値と対比される（ステップS10）N個の認証データが生成される。N個の認証データは、期待値の生成方法（図6，7）と同じ方法で生成される。

【0083】

このように認証データが生成されると、ステップS23において、ランダムチャレンジ受信制御部41は、通信部23を介して、RC受信メッセージを送信側の端末11に送信し、その旨を、応答メッセージ送信制御部44に通知する。

【0084】

ステップS24において、応答メッセージ送信制御部44は、これから受信する応答要求コマンドが何番目に受信されるものかを示すカウンタjに1を初期設定し、ステップS25において、応答メッセージ生成部43を制御して、カウンタjが示す順番に受信される応答要求コマンド（以下、第j番目に受信される応答要求コマンドと称する）に対応する認証データを組み込んだ応答メッセージを生成させる。

【0085】

次に、ステップS26において、応答メッセージ送信制御部44は、送信先の端末11から送信されてきた応答要求コマンドを（ステップS6）、通信部23を介して受信すると、ステップS27において、ステップS25で生成された第j番目に受信される応答要求コマンドに応じた認証データが組み込まれた応答メッセージを、通信部23を介して、送信側の端末11に送信する。これにより上述したように送信側の端末11で（ステップS10で）、第j番目に受信された（第i番目に送信された）応答要求コマンドに対応する認証データと、第i番目に送信された（第j番目に受信された）応答要求コマンドの期待値とが比較される。

【0086】

ステップS28において、受信側の端末11の応答制御部22の応答メッセージ送信制御部44は、送信側の端末11から送信される判定終了メッセージ（ステップS16）が受信されたか否かを判定し、受信されていないと判定した場合、ステップS29に進む。ステップS29において、応答メッセージ送信制御部44は、カウンタjを1だけインクリメントし、ステップS30で、カウンタj=N+1であるか否かを判定する。

【0087】

ステップS30で、カウンタj=j+1ではないと判定されたとき（すなわち、応答要求コマンドをN回受信されていないとき）、ステップS25に戻り、次に受信される応答要求コマンドに対して、それ以降の処理を実行する。

【0088】

ステップS28で、判定終了メッセージが受信されたとき、またはステップS30で、カウンタj=N+1であると判定されたとき（すなわち、応答要求コマンドがN回受信されたとき）、応答制御部22は、応答処理を終了する。

【0089】

以上のように、ランダムチャレンジから生成された認証データ（ステップS22）とその期待値（ステップS3）とに基づいて認証された受信側の端末11についてのみ応答時間に基づく通信距離の判別を行うようにしたので（ステップS10でNOの判定がなされた場合、ステップS11の処理がスキップされるので）、正規の機器のようになりすました機器にデータが送信されることを防止することができる（正規の機器のようになりすました機器が応答要求コマンドを受信し、応答要求メッセージを送信して、その機器にデータが送信されることはない）。

【0090】

また送信側の端末11で、応答要求コマンドに、新たに生成したランダムチャレンジを込み込んで受信側の端末11に送信し（ステップS6）、受信側の端末11で、応答要求コマンドを受信したとき（ステップS26）、予め生成された認証データ（ステップS22）と、その応答要求コマンドに組み込まれたランダムチャレンジとを連結して、または両者の論理演算を行って新たな認証データを生成し、それを組み込んだ応答メッセージを

返信することもできる（ステップ S 27）。なお送信側の端末 11 では、ステップ S 10 で新たな認証データと比較される期待値が、ステップ S 3 で生成された期待値と、応答要求コマンドに組み込まれたランダムチャレンジと連結されて、または両者の論理演算が行われて生成される。

【0091】

このように応答要求コマンドに組み込んだランダムチャレンジを利用して認証データおよび期待値が生成されるようにすることで、受信側の端末 11 は、送信側の端末 11 からの応答要求コマンドを受信した後でなければ、応答メッセージを送信することができなくなる。したがって、応答時間を短縮するために、応答要求コマンドを受信する前に応答メッセージを送信するなどといった不正行為を防止することができる。

【0092】

また、以上のように、受信側の端末 11 において、応答要求コマンドを受信する前に、認証データおよびそれが組み込まれた応答メッセージを生成するようにしたので（ステップ S 22, S 25）、応答要求コマンドを受信した後直ちに応答メッセージを送信側の端末 11 に返信することができる（ステップ S 27）。

【0093】

例えば、応答要求コマンドを受信した後に、認証データおよび応答要求メッセージを生成するようになされている場合、送信側の端末 11 で計測される応答時間に、その処理にかかる時間が含まれてしまうので、通信時間としての応答時間を正確に計測することができない。しかしながら本発明のように応答要求コマンドを受信した後直ちに応答メッセージを送信することができるようにしておくことにより、通信時間としての応答時間を正確に計測することができる。

【0094】

上述した一連の処理は、ハードウェアにより実現させることもできるが、ソフトウェアにより実現させることもできる。一連の処理をソフトウェアにより実現する場合には、そのソフトウェアを構成するプログラムがコンピュータにインストールされ、そのプログラムがコンピュータで実行されることにより、上述した送信可否判定部 21 および応答制御部 22 が機能的に実現される。

【0095】

図 8 は、上述のような送信可否判定部 21 および応答制御部 22 として機能するコンピュータ 101 の一実施の形態の構成を示すブロック図である。CPU (Central Processing Unit) 111 にはバス 115 を介して入出力インタフェース 116 が接続されており、CPU 111 は、入出力インタフェース 116 を介して、ユーザから、キーボード、マウスなどよりなる入力部 117 から指令が入力されると、例えば、ROM (Read Only Memory) 112、ハードディスク 114、またはドライブ 120 に装着される磁気ディスク 131、光ディスク 132、光磁気ディスク 133、若しくは半導体メモリ 134 などの記録媒体に格納されているプログラムを、RAM (Random Access Memory) 113 にロードして実行する。これにより、上述した各種の処理（例えば、図 5 のフローチャートにより示される処理）が行われる。さらに、CPU 111 は、その処理結果を、例えば、入出力インタフェース 116 を介して、LCD (Liquid Crystal Display) などよりなる出力部 118 に必要に応じて出力する。なお、プログラムは、ハードディスク 114 や ROM 112 に予め記憶しておき、コンピュータ 101 と一体的にユーザに提供したり、磁気ディスク 131、光ディスク 132、光磁気ディスク 133、半導体メモリ 134 等のパッケージメディアとして提供したり、衛星、ネットワーク等から通信部 119 を介してハードディスク 114 に提供することができる。

【0096】

なお、本明細書において、記録媒体により提供されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0097】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【図面の簡単な説明】

【0098】

【図1】 本発明を適用した情報通信システムの利用例を示す図である。

【図2】 図1の端末の構成例を示すブロック図である。

【図3】 図2の送信可否判定部の構成例を示すブロック図である。

【図4】 図2の応答制御部の構成例を示すブロック図である。

【図5】 送信可否判定処理および応答処理を説明するフローチャートである。

【図6】 期待値および認証データの生成方法を説明する図である。

【図7】 期待値および認証データの他の生成方法を説明する図である。

【図8】 パーソナルコンピュータの構成例を示すブロック図である。

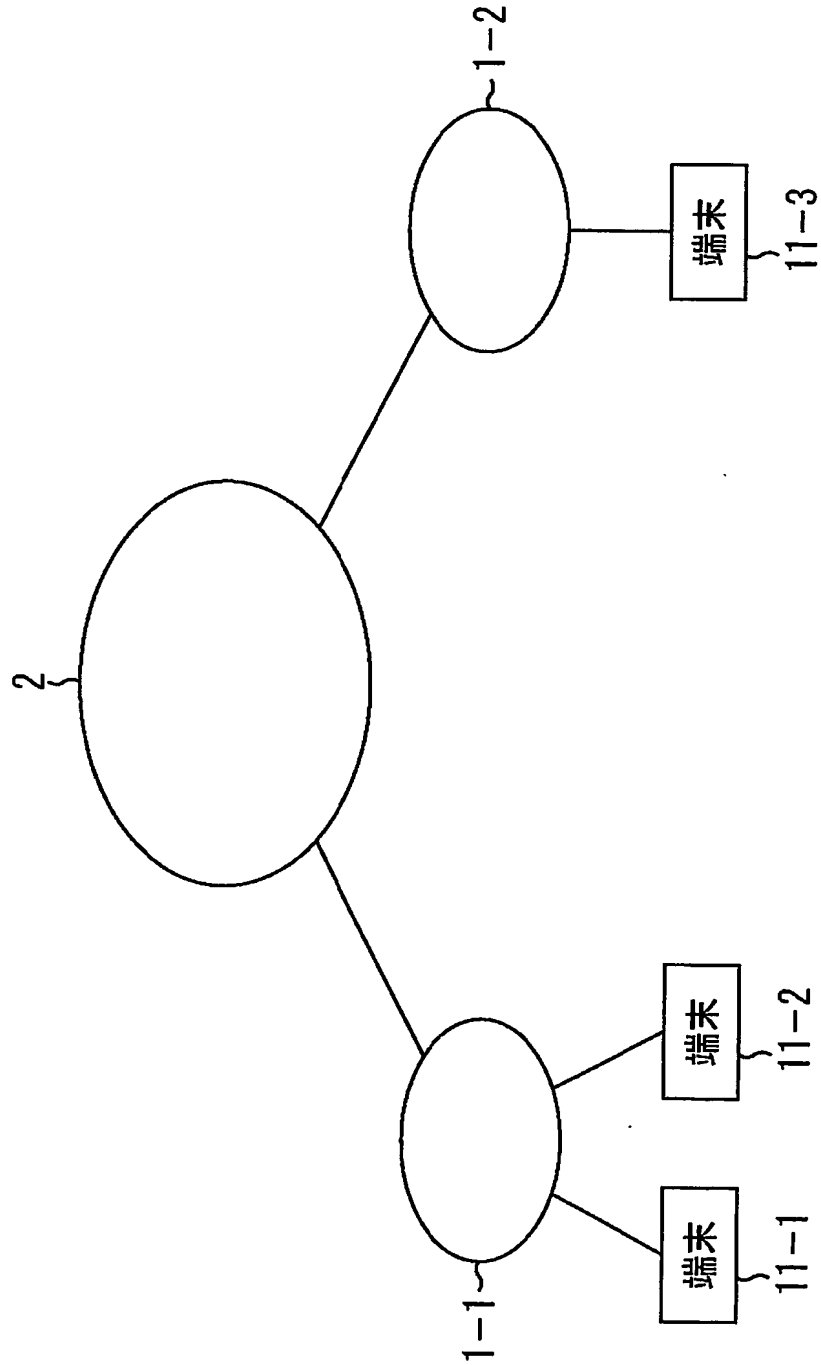
【符号の説明】

【0099】

1 LAN, 2 WAN, 11 端末, 21 送信可否探偵部, 22 応答制御部, 23 通信部23, 24 送信データ格納部, 31 ランダムチャレンジ生成部, 32 ランダムチャレンジ送信制御部, 33 期待値生成部, 34 コマンド送信制御部, 35 判定部, 36 応答時間計測部

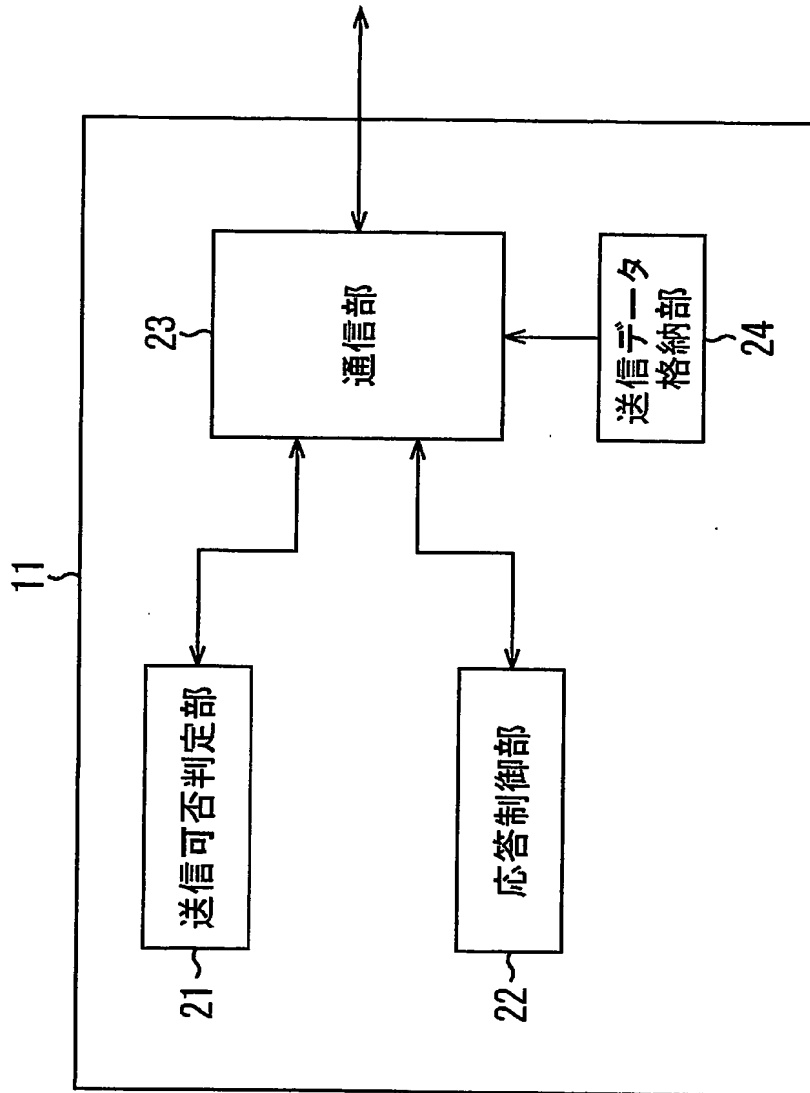
【書類名】図面
【図 1】

図 1



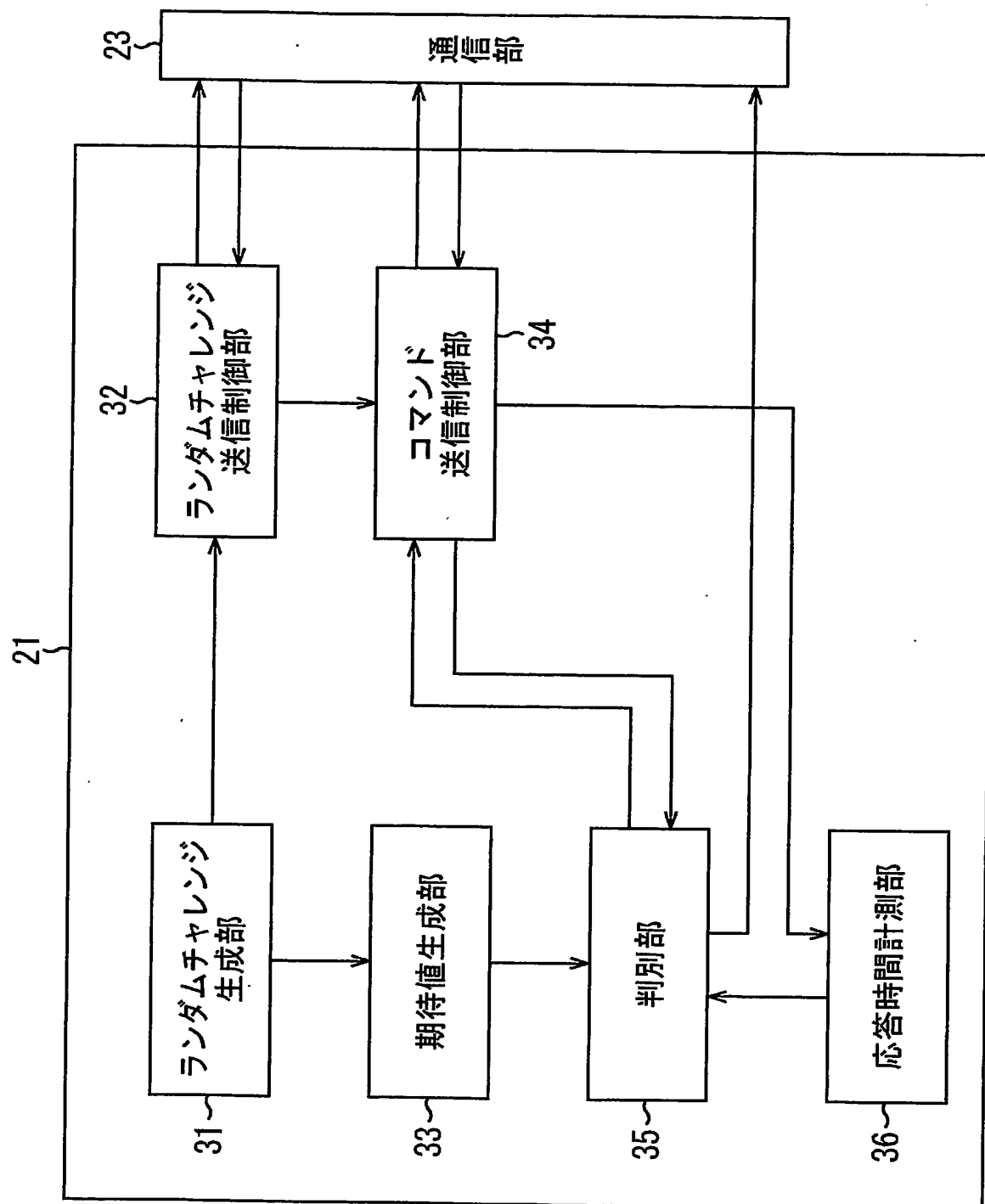
【図 2】

図2

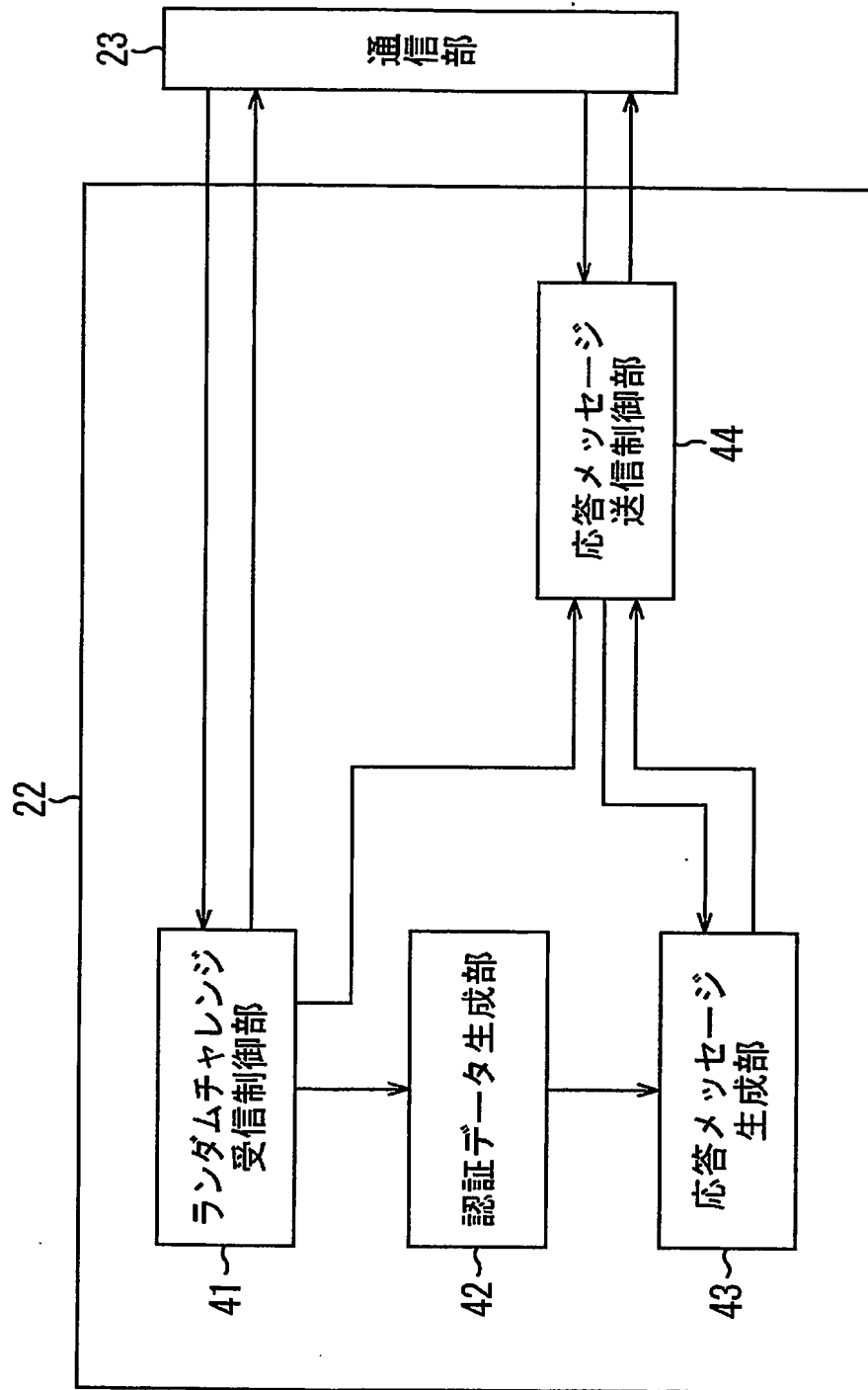


【図 3】

図3

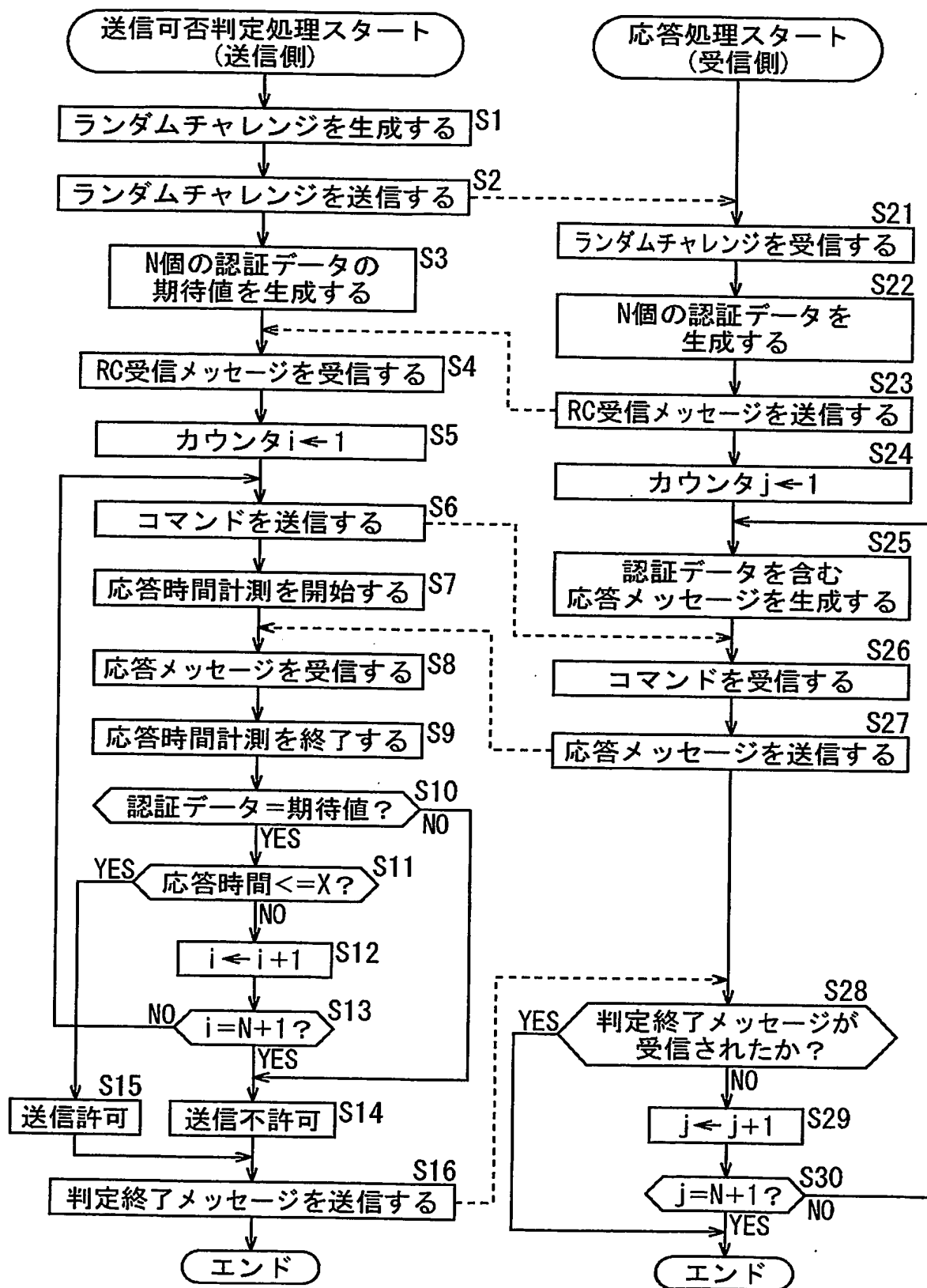


【図 4】
図4

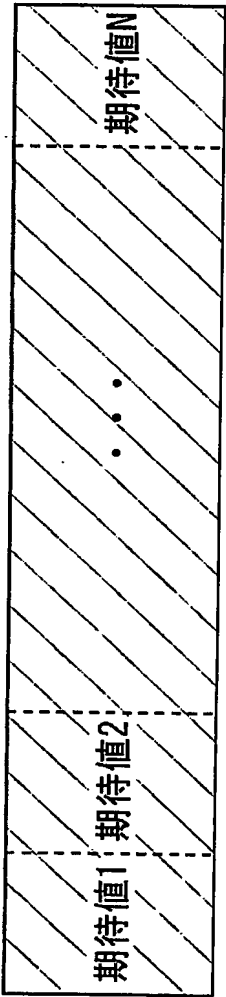


【図 5】

図5

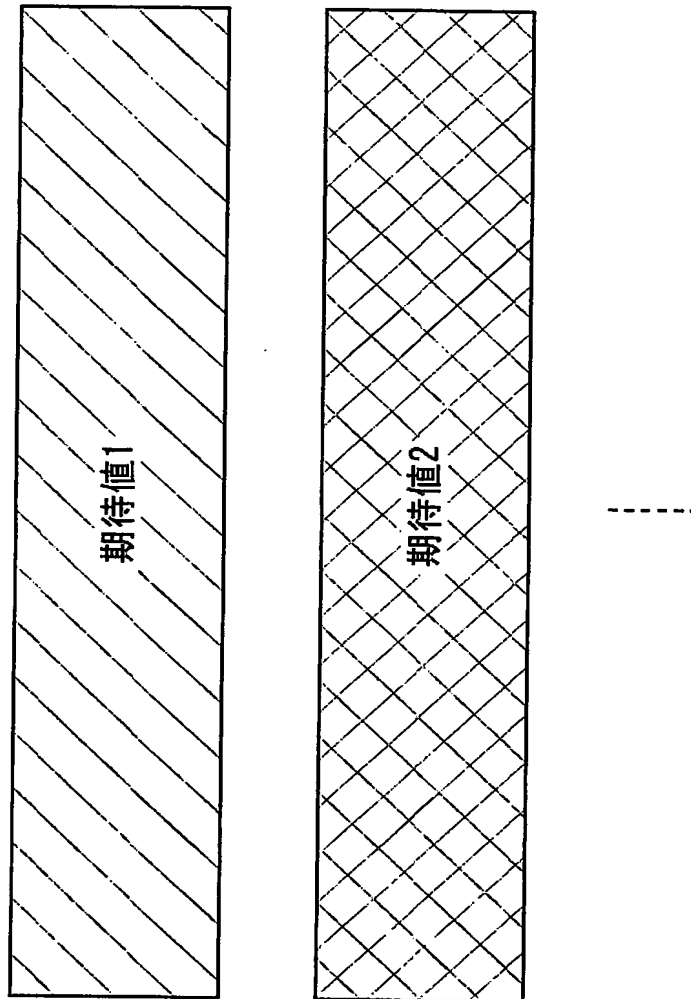


【図 6】
図 6



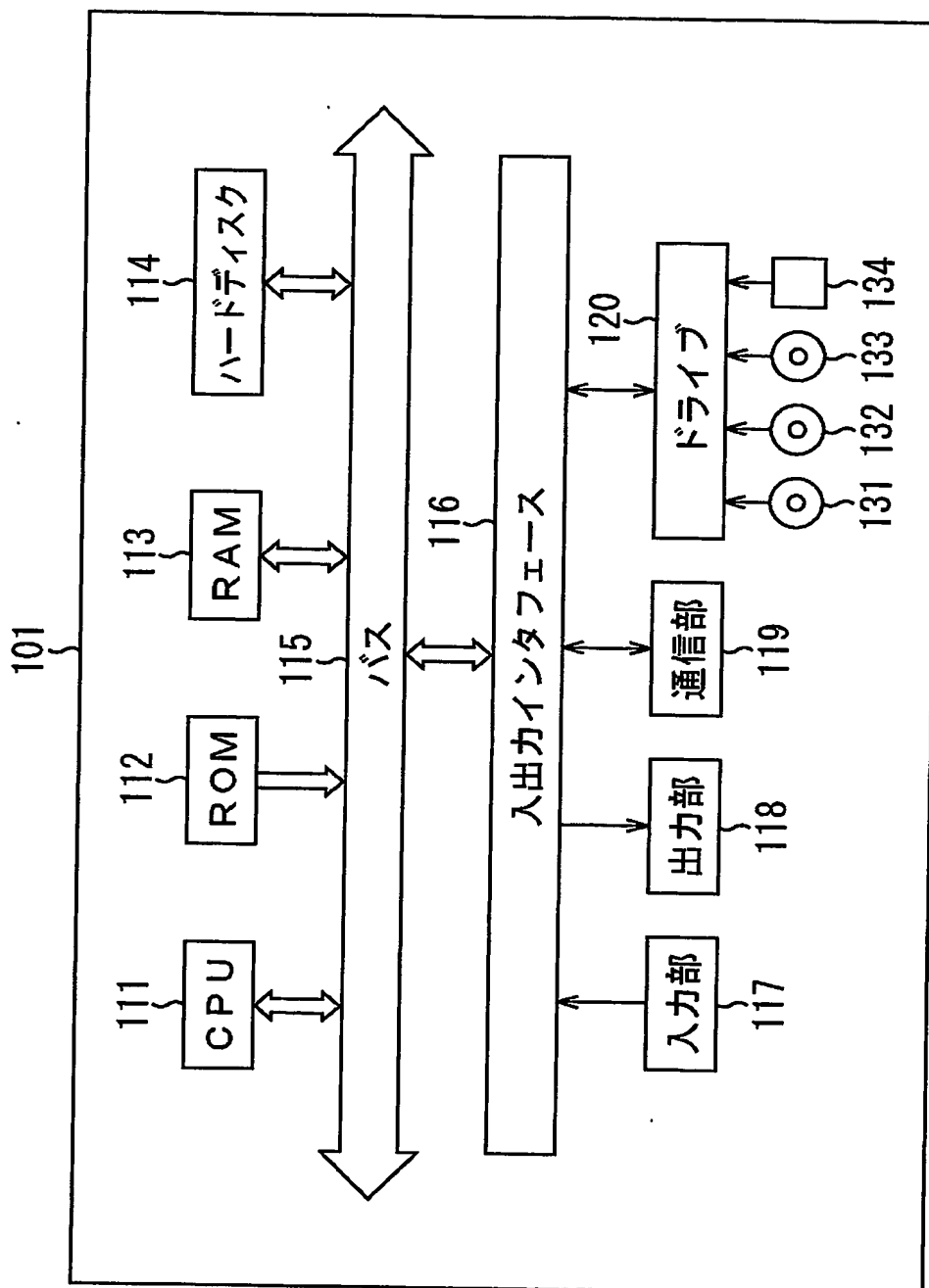
【図7】

図7



【図 8】

図8



【書類名】要約書

【要約】

【課題】通信時間を適切に計測することができるようにする。

【解決手段】受信制御部 41 は、送信側の端末 11 から送信されてきたランダムチャレンジを受信し、生成部 42 に供給する。受信制御部 41 はまた、ランダムチャレンジを受信した旨を表す RC 受信メッセージを、送信側の端末 11 に送信する。生成部 42 は、供給されたランダムチャレンジに対して、送信側の端末 11 における場合と同様のハッシュ処理を施し、その結果得られた認証データを生成部 43 に供給する。送信制御部 44 は、送信側の端末からの応答要求コマンドを受信する前のタイミングで、生成部 43 を制御して、受信する応答要求コマンドに対応した認証データを含む応答メッセージを生成させるとともに、応答要求コマンドを受信したとき、予め生成したその応答メッセージを送信先の端末に送信する。本発明は、コンテンツ提供システムに適用することができる。

【選択図】図 4

特願 2 0 0 3 - 2 8 1 3 4 8

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 2 1 8 5]

1. 変更年月日
[変更理由]

1 9 9 0 年 8 月 3 0 日

新規登録

住 所
氏 名

東京都品川区北品川 6 丁目 7 番 3 5 号
ソニー株式会社